ORIGINAL

EX PARTE OR LATE FILED

KECK, MAHIN & CATE

1201 NEW YORK AVENUE, N.W.
WASHINGTON, D.C. 20005-3919
(202) 789-3400
FAX (202) 789-1158

FILE NUMBER 46158-002

DIRECT DIAL (202) 789-3419

December 7, 1993

By Hand

EX PARTE

Mr. William Caton
Acting Secretary
Federal Communications Commission
1919 M Street, N.W., Room 222
Washington, D.C. 20554

Re: CC Docket No. 92-77; Billed Party Preference

Dear Mr. Caton:

The Inmate Calling Services Providers Task Force ("ICSPTF") wishes to respond to MCI Telecommunications ("MCI") ex parte letter dated October 25, 1993, in support of billed party preference ("BPP") for inmate calling services ("ICS"). As discussed below, MCI's proposed solution to the problems associated with BPP in the inmate calling environment would require the Commission to order drastic, costly and intrusive measures throughout the telecommunications industry. Moreover, even if the Commission took those necessary actions, there are several reasons why MCI's hypothetical solution would not be as effective at preventing inmate fraud and calling abuse than the inmate calling systems currently in place.

"Fraud Control" vs. "Call Control"

At the outset, ICSPTF wishes to address a flawed dichotomy raised by MCI regarding the function of inmate calling systems. MCI attempts to draw a distinction between "fraud control" measures and "call control" measures for the apparent purpose of implying that fraud control will continue to exist after BPP regardless of whether or not ICS providers are able to continue to provide premises-based call control functions. Apparently, MCI realizes the difficulty of assuring premises-based call control

functionality after BPP.[1] It suggests that call control features after BPP could more predominately become network-based (i.e., will be supplied by IXCs) rather than the premises-based systems currently in place. (The fallaciousness of this assertion is addressed below.)

MCI defines "fraud prevention" as "the process of preventing the unauthorized use of a carriers [sic] network with the intent not to pay for that use." "Call control," on the other hand, is defined by MCI as "method[s] to enhance an institution's administrative capabilities to monitor and restrict the calling privileges of inmates." MCI goes on to suggest that fraud

---

[1] MCI states that "[t]oday all switched access calls originating at an individual institution are routed to a single carrier using presubscription. This allows the prison to work with a single carrier to determine what call controls will be applied and to administer changes in either the desired call control features or the control parameters." In a calculated understatement, MCI then goes on to concede that "[BPP] may affect the way call control systems are designed and administered." What this statement in essence translates into is MCI's recognition that ICS providers will, under any plausible BPP scenario, cease to provide the equipment necessary for call control. The economic incentives to do so will completely disappear.

Indeed, ICSPTF has, on several occasions, explained why BPP will take away the incentive of ICS providers to continue to provide inmate calling systems. ICS providers generally recover the costs for their equipment by servicing inmate calls from origination to termination, and following through with the billing and collection. Under this system, ICS providers maintain total financial responsibility for inmate calls. ICS providers thus have an incentive to prevent fraud at every turn. For obvious reasons, BPP will obliterate this form of cost recovery. While there may be theoretical solutions for alternative cost recovery mechanisms under BPP, such as state appropriations or the tariffing of ICS equipment, for practical reasons these solutions will not work. The tariffing of ICS equipment will ultimately serve to <u>increase</u> the cost of inmate calls -- a result that is contrary to the underlying purpose of BPP. And given the already intense financial pressures facing states with regard to the funding of the basic infrastructure needs of correctional institutions, the appropriation of additional funds for specialized inmate phone equipment throughout all 50 states is highly unlikely.

prevention measures will continue to exist whether or not correctional authorities and/or IXCs determine how, and if, they will implement call control functionality after the ICS provider leaves.

MCI has drawn an artificial distinction. The so-called "call control" features that MCI describes (i.e., call monitoring, call recording, 3-way detection and blocking, etc.) ultimately serve to reduce fraud. They are not, as MCI suggests, solely "to protect the general public from the potential of abusive calls." For example, call velocity monitoring -- a feature that MCI defines as "call control" -- allows the ICS provider to detect unusual calling volumes to a particular number, and thus allows the ICS provider to detect and control subscriber fraud as soon as possible. Moreover, MCI is clearly wrong to the extent that MCI suggests that billed number screening ("BNS") and line identification data base ("LIDB") queries are "call control" features. BNS and LIDB queries have the sole purpose of deterring fraud.

Indeed, MCI's own letter recognizes that the features its describes as "call control" ultimately serve to prevent fraud. MCI states that "the fraud prevention techniques such as velocity, dollar value, or time duration algorithms . . . are valuable tools to detect and prevent fraud." Thus, it is clear that MCI's attempt to draw a distinction between fraud control and call control is, for all practical purposes, illusory. The call control features that ICS providers currently provide serve a valuable fraud control function. They are equivalent in meaning and in purpose to "fraud control." The exit of ICS providers who currently provide these call control features after BPP is implemented will be detrimental to the overall fraud prevention effort at correction institutions.

Moreover, MCI discounts the social value of the "call control" features that do have the primary purpose of protecting "the general public from the potential of abusive calls." Clearly, the victims of an inmate's crime, the jurors who convict inmates and the judges and attorneys involved in the criminal judicial process support a system that prevents abusive calling by inmates. The premises-based systems that ICS providers install and operate -- and which will not survive under BPP -- provide a valuable public service by deterring such abusive calls.

The Implementation of a Network-Based Call Control System Would Require The Commission To Take Drastic and Intrusive Measures.

Before turning to the inherent problems with a network-based call control system, there is a fundamental -- and troublesome -- point that MCI has failed to mention. Under MCI's scenario, the Commission would be forced to take several drastic and intrusive actions, whose costs are at present unknown and have not been included in the already enormous cost of implementing BPP, in order for a network-based call control system to work.

First, the Commission would have to order every IXC throughout the nation to implement network-based control features. Indeed, as MCI explains, except for MCI, "no other [IXC] offers inmate call control systems using a centralized network solution such as MCI's." However, BPP will require prison traffic to be routed to a multitude of IXCs, not just MCI. Thus, in order for MCI's scenario to be effective, universal implementation of the network-based control systems would be required. Moreover, as discussed below, a network-based call control system can only be effective if there is a means to ensure daily interaction between every IXC and every correctional institution throughout the nation. The only way to ensure these results is for the Commission to use its mandate powers.

This is not the only intrusive measure the Commission would be forced to take. As MCI admits, the ANI "29" II digit sequence is not universally available. Many LECs, particularly those existing in the rural areas where prisons are frequently located, do not offer or do not have the capability to carry that ANI code, either as a class of service code or as a "Flex ANI" offering. Nevertheless, the provision of the ANI code "29" from the LECs to the IXCs is a fundamental component of a network-based call control system. Thus, the Commission would also be forced to mandate that every LEC throughout the country upgrade their facilities to have the capability to provide the "29" ANI digit code as part of its inmate offering.

Third, MCI assumes that the LEC will conduct a BNS query on every call. There is no reason, however, for the LEC to conduct any inquiry other than to determine carrier identification (i.e., the carrier to whom a call is to be routed) on interLATA calls. That is all the LEC is paid for under BPP. Thus, MCI's scenario would require the Commission to order every LEC throughout the nation to conduct a BNS inquiry for interLATA calls.

ICSPTF is currently attempting to gather data to show what it will cost for the Commission to order universal implementation of network-based control systems, including a means for daily interaction between every IXC and every correctional facility throughout the nation, and what the cost will be for the Commission to order every LEC throughout the nation to offer ANI digit "29" and conduct interLATA BNS. While ICSPTF will provide the Commission with such data when the data is available, at this point it is clear that these costs would likely range in the tens of millions of dollars. Of course, these costs would add to the approximately $1.5 billion that the implementation of BPP is already expected to cost.

The Inherent Problems With a Network-Based Call Control Solution

There are two primary reasons why a network-based call control system in a BPP environment cannot be as effective as a premises-based system at preventing inmate fraud and abuse. First, the call routing process under BPP requires a multiplicity of steps, an increased numbers of participants, and there is an increased potential for malfunctions. This means that there will be increased opportunities for fraud.

For example, one of the most troublesome aspects of MCI's scenario is the fact that it would be necessary to have no fewer than three database queries for inmate calls, rather than the single database dip currently conducted by the ICS provider.[2] The

---

[2] MCI's diagram entitled, "BPP Prison Collect Calling Via Phone Service Provider (Network-Based)" is the only post-BPP diagram that is relevant and therefore warrants discussion. Indeed, MCI's diagram entitled "BPP Prison Collect Calling Via Inmate Phone Service Provider (Premised-Based)," is wholly irrelevant to the analysis since, as discussed above, ICS providers will have no incentive to continue providing premises-based services after BPP. Moreover, to the extent that MCI seriously believes that premises-based systems can continue to exist after BPP, its diagram contains a major defect that renders it meaningless. That is, MCI shows inmate calls being converted from a 0+ call to a 1+DDD call after leaving the premises. Conversion of 0+ to 1+ calling is, of course, a feature of current inmate calling systems. Thus, under MCI's diagram, the call would be serviced by the premises-based phone provider, not by the carrier of the billed party. This is in conflict to the whole purpose of

first database dip would occur when the call and other information reached the serving LEC central office identifying itself as an operator-assisted call. At that point the LEC would conduct a carrier identification inquiry in order to determine where to route the call. Once the carrier had been correctly identified and the information transmitted to the relevant node in the LEC network, the call would be routed to the IXC along with the ANI, the terminating number and, if everything is working right, the ANI II digits.

Upon reaching the IXC network, the call will, presumably, be accompanied by the ANI digits, most likely 07. This will spark the second database query necessary to process the call, since the 07 digits merely mean that "alternate billing information is required." Therefore, the IXC must ascertain the billing restrictions associated with that originating line.[3] To ascertain the billing restrictions, the IXC will be required to dip into a database which is provided by, and presumably kept up to date by, the LEC. This assumes, of course, that the IXC in fact subscribes to this database and the IXC's operators have been instructed to perform the database look-up.[4]

Presumably, if the database is up to date, and the IXC subscribes to the proper screening databases, and has procedures in place, the IXC will then find out the call is collect only. The IXC must then conduct the third database query in order to determine whether there is any billing restriction on the terminating number.

Of course, in the current environment, the ICS provider performs all these functions with a single database dip. There is no need to ascertain the relevant carrier since the ICS provider

---

BPP. Indeed, under BPP the call must come into the LEC office as a 0+ call in order for the LEC to route the call to the billed parties' carrier. There is simply no other way for BPP to work.

[3] As discussed above, MCI's scenario would require the universal offering of ANI II digits "29," but at present very few LECs offer ANI digits "29," and it is unclear whether this new service will ever be universally available.

[4] As has been discussed elsewhere throughout this proceeding, IXCs often do not subscribe to these databases for various economic and business-related reasons.

is the one financially responsible for servicing the call. Moreover, there is no need for a database dip to determine the billing restrictions on the originating line since the ICS provider already knows that all calls are on a collect basis. The only database query the ICS providers needs to do is to ascertain whether there is a billing restriction on the terminating number.

The multiple steps and actors associated with processing a call in the BPP environment introduce opportunities for error and/or negligent conduct which, in turn, provides more opportunity for fraud. For example, it is well known throughout the industry that the transmission of ANI II digits from the LEC to the IXC is anything but a perfect process. Errors often occur. Moreover, not all IXCs are capable of receiving full information from the LECs. Even when the correct ANI II digits are transmitted and the IXC's equipment is capable of receiving full information, the IXC must be willing to take responsibility for executing the steps necessary to make sure the process works. The multiplicity of steps involved, the increased numbers of participants, and the potential for malfunctions means that there will be increased opportunities for fraud under the complex routing system that BPP requires.

The second major problem with a network-based control system is that the IXCs will not be able to communicate on a daily basis with every correctional facility throughout the nation in order to receive information that is necessary to prevent fraudulent or abusive calling before it is too late. Indeed, one of the most important reasons why premises-based ICS providers are able to prevent inmate fraud and abusive calling in a timely manner is because ICS providers interact on a daily basis with the correctional facility they serve. Through these daily interactions, ICS providers discover -- at the earliest possible moment -- unusual calling patterns and other pertinent information which allows the ICS provider to take immediate corrective action.

Indeed, even MCI has recognized the need for daily interaction with the facility in order for its network-based control system to be effective. As the enclosed sales literature of MCI reflects, an important component of MCI's system is its use of an "On-site Administrator." The "On-site Administrator" provides the correctional facility with "daily automatic recovery" of pertinent information used to detect and prevent fraud and abusive calling. Of course, even assuming that every IXC implements a network-based call control system, it would be extremely difficult, if not impossible, for every IXC to have an information sharing arrangement with every correctional facility throughout the nation.

As discussed above, the Commission would be forced to exercise its mandate powers and order such arrangements -- an unlikely occurrence. Therefore, for practical reasons, the use of network-based call control systems under BPP will not be as effective as the premises-based systems that ICS providers currently provide.

There is another flaw in MCI's letter that needs to be addressed. MCI implies that fraud prevention could possibly become more effective under BPP than under the current system. MCI tries to suggest that since under the current system there are multiple carriers that "deliver collect calls to the same billing number," there is a possibility of fraud that goes unchecked. More specifically, MCI states

> Lack of visibility to all calls billed to a collect calling termination prevents carriers from applying the fraud prevention techniques such as velocity, dollar value, or time duration algorithms that are valuable tools to detect and prevent fraud. Since collect calls to an individual billing number are spread across a multitude of carriers it eliminates the ability of each of those carriers to adequately monitor and audit the billing history of the billed party. . . . Further, once fraud is detected the current system encourages carrier hopping or subscription fraud by the billed party, starting the cycle over again.

Although subscription fraud by inmates is a significant concern, MCI's concern is completely misplaced. Carrier hopping is a concern under BPP, not the current system. BPP will provide the incentive for the perpetrator outside the prison to "hop" from carrier to carrier as the collect calling limits are reached with each carrier. Under the current system, the ICS provider controls the IXC selection process. Thus, MCI has taken one of the vulnerabilities of BPP and inappropriately misapplied it to the current system.[5]

---

[5] MCI's example of subscription fraud is somewhat unusual. The type of fraud that MCI is concerned about requires the perpetrator outside the prison to have an ongoing relationship with multiple prisoners in multiple locations and assumes that no single IXC is presubscribed to any two of those locations. By all

We stongly urge the Commission to pay close attention to the concerns that ICSPTF has raised herein and in its other filings in this proceeding. Regardless of the Commission's decision regarding BPP in general, the Commission must not allow BPP to be applied to inmate calling services.

Sincerely,

Albert H. Kramer
David B. Jeppsen
Counsel for the Inmate
Calling Services Providers
Task Force

AHK/hlh

Enclosure
cc: Gary Phillips
Mark Nadel

---

accounts, this is not a prevalent, or even likely, type of fraud. And even if it were a prevalent type of fraud, MCI assumes that under BPP all IXCs will independently adopt the call control functions currently provided by the ICS providers, clearly not a likely occurrence.

Control Is In-line With On-line Support

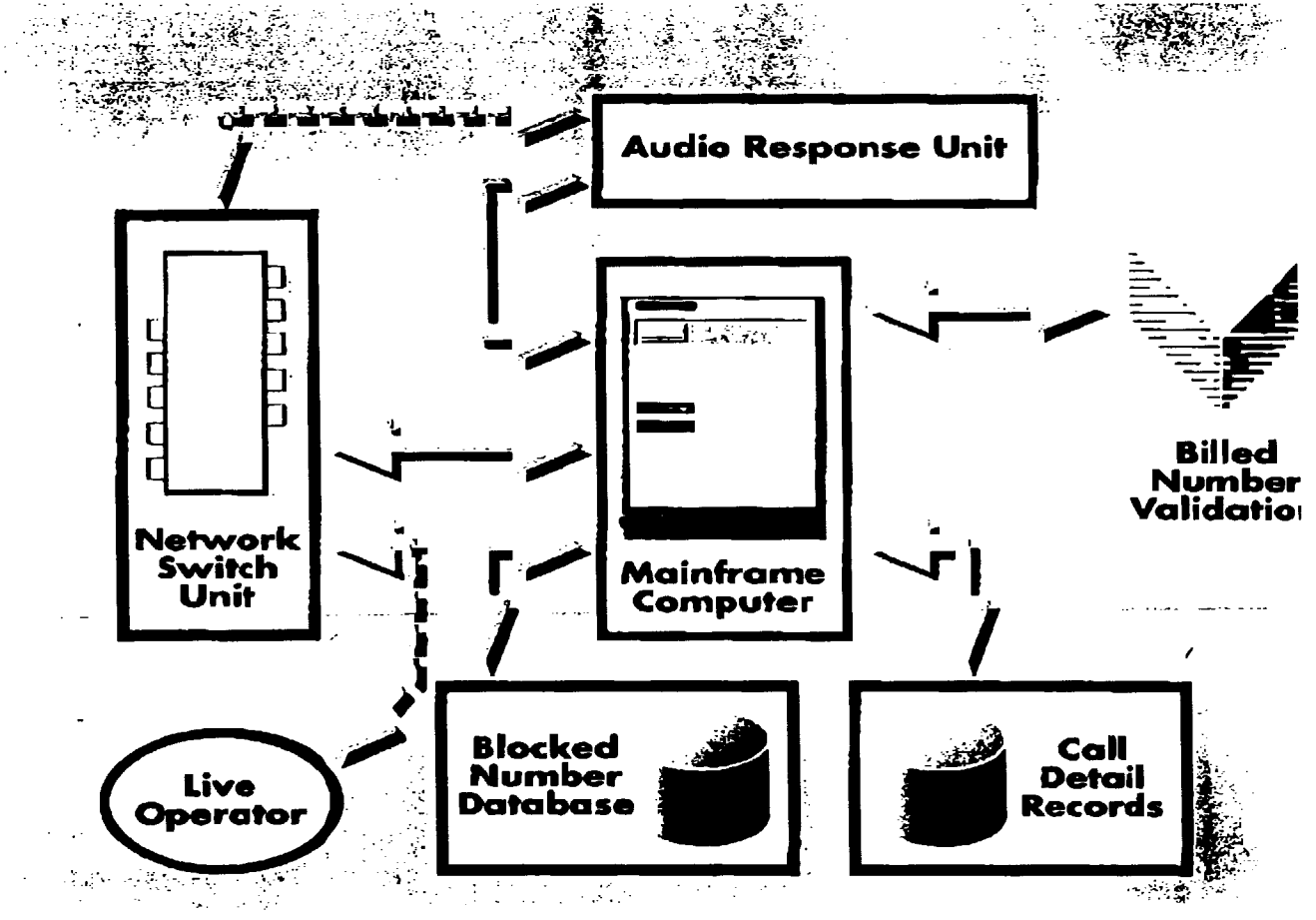
The Maximum Security On-site Administrator makes obtaining call records easy by using a simple selection menu. Customized reporting is available for daily automatic recovery of various menu-driven options such as:

- **Inmate Phone Report**– Breaks out call usage by originating number.
- **Frequently Called Number Report**– Shows most frequently called numbers using customer selected parameters.
- **Cell Block/Phone Correlation Report**– Identifies calls made to an identical number from different cell blocks and/or groups of phones. Also, detects two inmates calling an identical number, at the same time (conference calls), from the same institution.
- **Traffic Report** – Depicts hourly usage by phone or institution.
- **PIN Report** – Lists all PINs and associated call activity.
- **Search Report**– Allows the customer to "search out" call information by using specified parameters (phone number, PIN, date, time, call duration).
- **Commissions Report**– Quantifies commissions by originating facility and phone number. This is not accessible through The Maximum Security On-site Administrator software and is sent separately through MCI's internal systems.

Complete Security At Your Fingertips

MCI Maximum Security is the most advanced and efficient automated inmate call system availabl today. It is easy to use and provides the control an security you want. The Maximum Security On-sit Administrator allows prison officials to manage sys administration and call reports. When making a ca inmates are prompted through the calling process v a series of pre-recorded instructions. The destinati phone number is compared to several protection da bases to certify selected functionality or permissible called numbers. If the number fails certification, th call is blocked. If the number passes, the automate operator requests the inmate's name and processes the call. If the recipient accepts the call, the call is connected.

MCI Facility



MCI Maximum Security Puts You in Command

Flexible Options Tailored To Your Facility

MCI Maximum Security provides you with the tools to manage your inmate calling most effectively. You select the features needed to enhance your facility's phone system utility while extending your ability to control inmate behavior.

For example, you can select public abuse prevention features such as Number Restriction with an Allowed Call List utilizing a Personal Identification Number (PIN). Voice Overlay can be selected to announce randomly throughout the call conversation, that the call is from an inmate in a correctional facility.

Other options include:

- **Call Termination** – A way of controlling call duration automatically. This can be used as a behavior incentive.

- **Inmate Messenger Service** – An innovative MCI Maximum Security option that allows inmates to record a message for future delivery if the person being called is not available. This ensures that more calls are completed, adding to your revenue base.

Comprehensive Reporting - Your Key To Maximum Management Control

MCI's unique mainframe computer, network-based system guards all customer-selected feature intelligence and call records by maintaining the Maximum Security central database in MCI-controlled facilities. Through the use of The Maximum Security On-site Administrator, management of features is easy to perform. This system will allow both uploading of information (ie. PINs) and downloading of Call Detail Records (CDRs) for reporting. MCI offers standard and customized reports to provide the level of detail needed to manage your facility effectively.

MCI - A Total Solutions Provider

At MCI, we are dedicated to providing communication solutions tailored to correctional facilities. We take a cooperative approach in working with you to maximize inmate calling control and revenue potential.

Unsurpassed Reliability

MCI Maximum Security calls are transmitted on a dedicated subnetwork of the MCI intelligent network. This mainframe computer, network-based system has built-in redundancy for both lines and processing equipment. Employing the most advanced technology, such as alarms and instantaneous re-routing capabilities, the MCI network provides tremendous quality and reliability, assuring that your phone system will have maximum availability for inmate calling.

You receive information at your discretion using The Maximum Security On-site Administrator. Changes to your system, such as adding or deleting PINs, blocking a number, or customizing call reports, can be made easily and quickly even during periods of high traffic and understaffing. MCI Maximum Security's mainframe computer, network-based system ensures centralized database manipulations for all your facilities at the same time. At your choice, changes are made within minutes.

MCI

Unrivaled Customer Support

As an established leader in the telecommunications industry, with one of the largest networks in the world, MCI is committed to giving you continued support. We deliver the superior support your facility demands by assigning a team of dedicated professionals who are trained in the needs of correctional facilities. From our correctional facility system engineers to our account representatives, MCI is committed to providing maximum security and maximum value.

Secure Your Facility Today

For more information on how MCI can help you lock in superior service and support, contact your MCI Account Team. Maximum value is available today with MCI Maximum Security. Call 1-800-47-PRISON.

MCI MAXIMUM

MCI Maximum Security®. The Only Mainframe Computer, Network-based System Available Today